



Compliance & Risks

Webinar

# Medical Devices in the Age of AI and Cybersecurity: Regulatory Insights

19 November, 2025



→ | [complianceandrisks.com](https://complianceandrisks.com)



Q&A  
Session

Slides &  
Webinar  
Recording



Request a  
Demo

# Webinar Platform Tips



Compliance & Risks

# Meet the Team



Fernanda Paro  
Senior Regulatory  
Compliance Specialist



Patricia Weathers  
Regulatory  
Compliance Specialist



Kahyeon Seo  
Regulatory  
Compliance Analyst

# Mission Statement

Ensure global companies have the tools & information to build safe, sustainable, products in a world full of change

# Trusted by the World's Leading Brands

**SAMSUNG**

**Miele**

 **MOTOROLA**

**EPSON®**



 **Abbott**

**FUJITSU**

**BOSE**

**BELDEN**

**PHILIPS**

**logitech**

**XEROX®**

**Thermo**  
SCIENTIFIC

  
**PUMA**

**GARMIN** 



Compliance & Risks



100K<sup>+</sup>  
Regulations

195  
Countries

10<sup>+</sup>  
Industries

28  
Languages

30  
Global  
Network  
Partners

9.6k  
Expert  
Queries  
answered



WHAT WE DO

# Unlocking Market Access

Keep on top of regulatory changes and their impact worldwide. Early warning alerts, impact probability, productivity workflow tools and so much more.





The digital transformation of healthcare, regulatory convergence and why compliance is now a strategic enabler for MedTech innovation.



# Integration of digital technologies: data, software, connectivity, and automation

Into all aspects of care delivery and health-system operations. Specifically for medical devices, it is reshaping design, functionality, risk management & post-market oversight.

## Key Drivers:

- Software-based and AI-enabled devices
- Software as a Medical Device - SaMD, machine learning, cloud computing, and data analytics.
- Connectivity and IoT (Internet of Medical Things)
- Devices increasingly communicate with each other and with clinical information systems.
- Demand for remote monitoring and telemedicine
- Especially accelerated by global health-system pressures and aging populations.
- Real-world evidence (RWE)
- Continuous data generated by connected devices is valuable for safety, performance, and regulatory decisions.
- Cybersecurity requirements
- As devices connect to networks, they introduce new risks that must be managed across the lifecycle.

## Examples:

- Wearables used for chronic-disease management (e.g., cardiology, diabetes).
- AI-based radiology diagnostic tools.
- Smart infusion pumps with remote alerting.
- Cloud-connected surgical robots.
- Predictive analytics built into home-based devices.

The impact: devices become more intelligent, adaptive, and data-driven, but also more complex to regulate.

# Regulatory Convergence in Medical Devices

## Meaning

### Why Convergence is Needed

- Faster Access to Safe Medical Devices
- Reduced Burden for Manufacturers
- Improved Patient Safety and Quality

### Key Elements

- Harmonized Definitions & Risk Classification - Using aligned device definitions and risk-based rules (e.g., low, medium, high risk).
- Standardized Technical Documentation - The IMDRF (International Medical Device Regulators Forum) developed the Table of Contents (ToC) for technical files.
- Recognition of International Standards: ISO 13485 (Quality Management System), ISO 14971 (Risk Management), IEC 60601 series (Electrical safety)
- Reliance & Recognition Mechanisms: Some regulators accept or partially rely on: FDA approvals, EU CE marking, TGA/Health Canada decisions - This avoids duplicate work.
- Post-market Alignment - Including vigilance reporting formats and adverse event terminology (e.g., IMDRF codes).

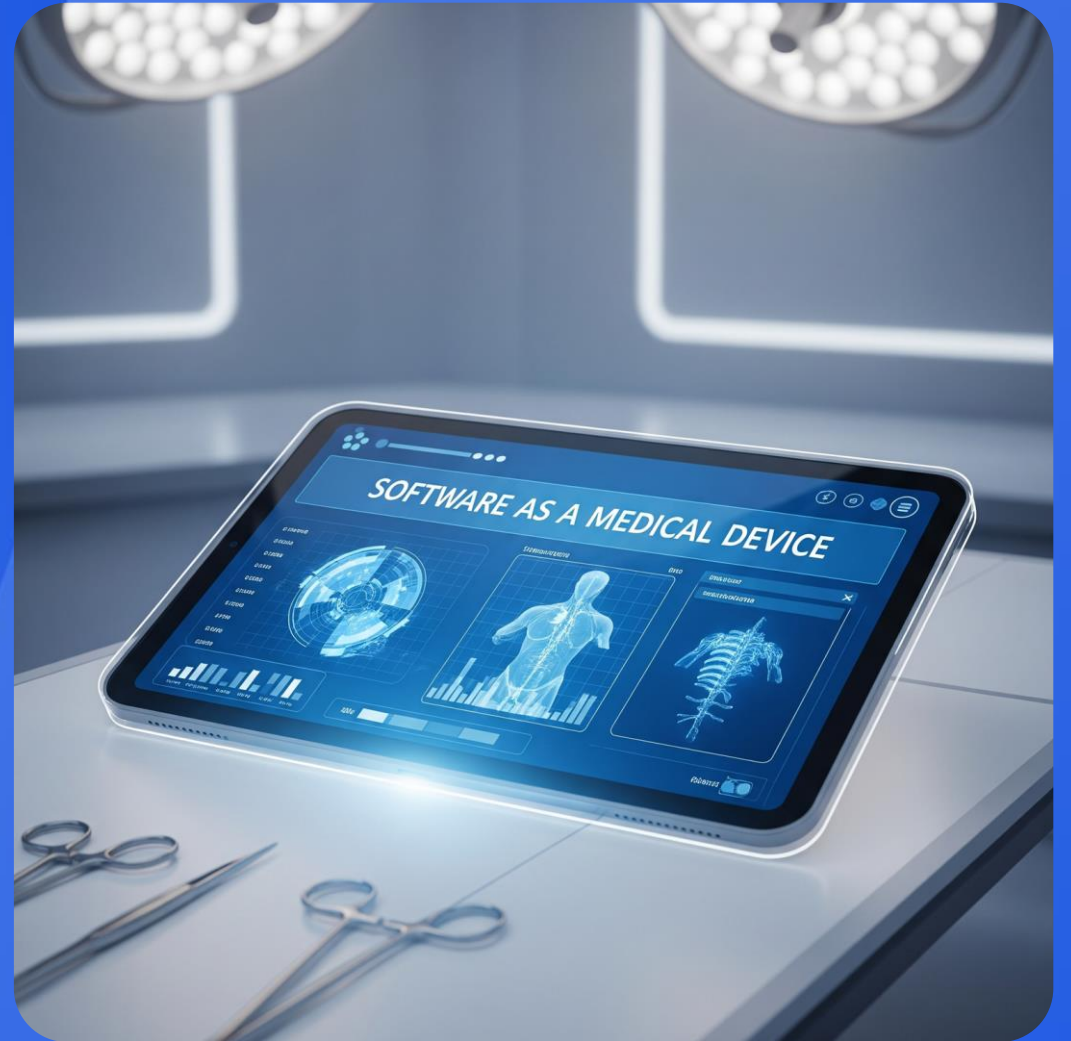




Compliance & Risks

# AI in Medical Devices

Legal & Regulatory Frameworks



→ | [complianceandrisks.com](https://complianceandrisks.com)

# Software as a Medical Device (SaMD) vs. Software in a Medical Device (SiMD)



## Software as a Medical Device (SaMD)

Definition: Software with a medical purpose, independent of a physical device.

Platform: Runs on general platforms (e.g., cloud, phone, tablet).

Regulation: Regulated as a standalone medical device.

Example: AI algorithm on a server analyzing MRI scans.



## Software in a Medical Device (SiMD)

Definition: Software that is integral to a physical medical device.

Platform: Embedded in or controls specific hardware.

Regulation: Regulated as part of the overall hardware system.

Example: Firmware controlling an insulin pump or ventilator.



# AI Risk Classification: EU AI Act & IMDRF

## EU AI Act Classification



- High-Risk: Most AI-driven medical devices. Triggers strict compliance (QMS, documentation, transparency).
- Limited/Minimal Risk: e.g., administrative triage.
- Unacceptable Risk: Prohibited (e.g., social scoring).

## IMDRF Framework (SaMD)

4 Risk categories (I - IV) based on two axes:

- Significance of Information: (Inform, Drive, Diagnose)
- State of Healthcare Condition: (Non-serious, Serious, Critical)
- Example: AI diagnosing a critical condition = Highest Risk.

# AI Risk Classification: United States



## No Separate AI Risk

The FDA does not have a separate risk classification system \*for AI\*. Instead, it uses its existing device framework.



## Device-Based: Class I, II, III

AI-driven devices are classified as Class I, II, or III, just like any other medical device, based on their potential for harm.



## "Intended Use" is Key

The classification and regulatory pathway (510(k), De Novo, PMA) are determined by the device's specific intended use.



# FDA vs. EU: Regulating Adaptive AI

## FDA (United States)

### Approach: Adaptive TPLC Framework

- Grounded in Executive Orders and focused on risk management.
- Core Mechanism: Predetermined Change Control Plan (PCCP).
- Key Guidance: Good Machine Learning Practices (GMLP).
- A PCCP is a pre-approved plan outlining how an AI will learn, what changes are permitted, and how they will be validated post-market.

## European Union

### Approach: Dual Compliance Framework

- Mandates compliance with TWO complete sets of laws.
- 1. MDR/IVDR: Covers safety, performance, and clinical evidence.
- 2. AI Act: Covers data governance, technical documentation, transparency, and human oversight.



# AI Regulation in Asia: Key Approaches



## Prescriptive Frameworks

- South Korea (Digital Medical Products Act): Leads with a binding act. Mandates AI governance, data quality validation, and defenses against data poisoning.
- China (NMPA Guidance): Requires secure data training, traceability, and performance evaluation.  
\*Prohibits\* adaptive self-learning without re-approval.



## Harmonization & Guidance

- Japan (PMDA/MHLW): Favors a flexible approach. Aligns with global standards (like IMDRF/GMLP) over specific new MedTech AI laws.
- Taiwan (TFDA): Regulates under its general Medical Devices Act. Recommends following international standards, like the FDA's GMLP.

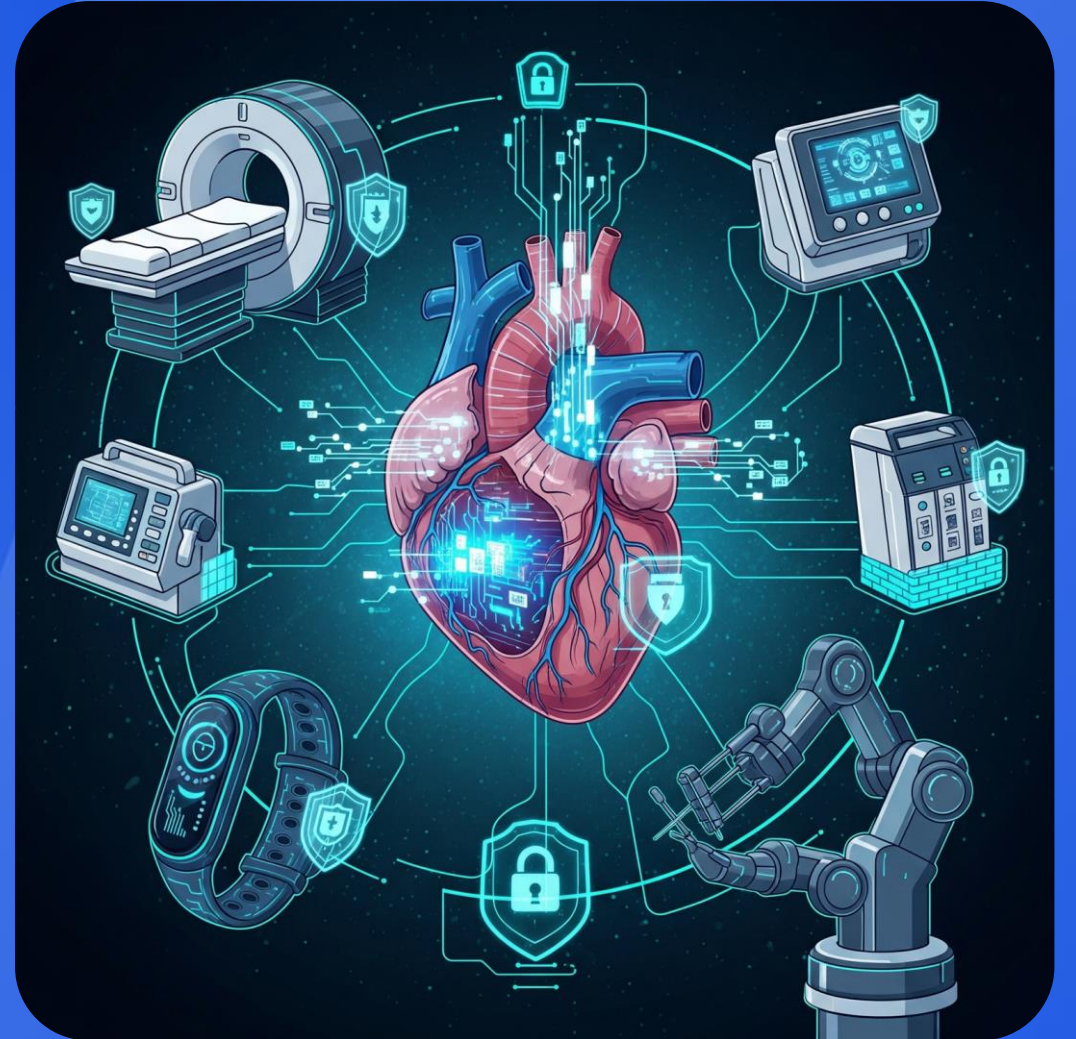




Compliance & Risks

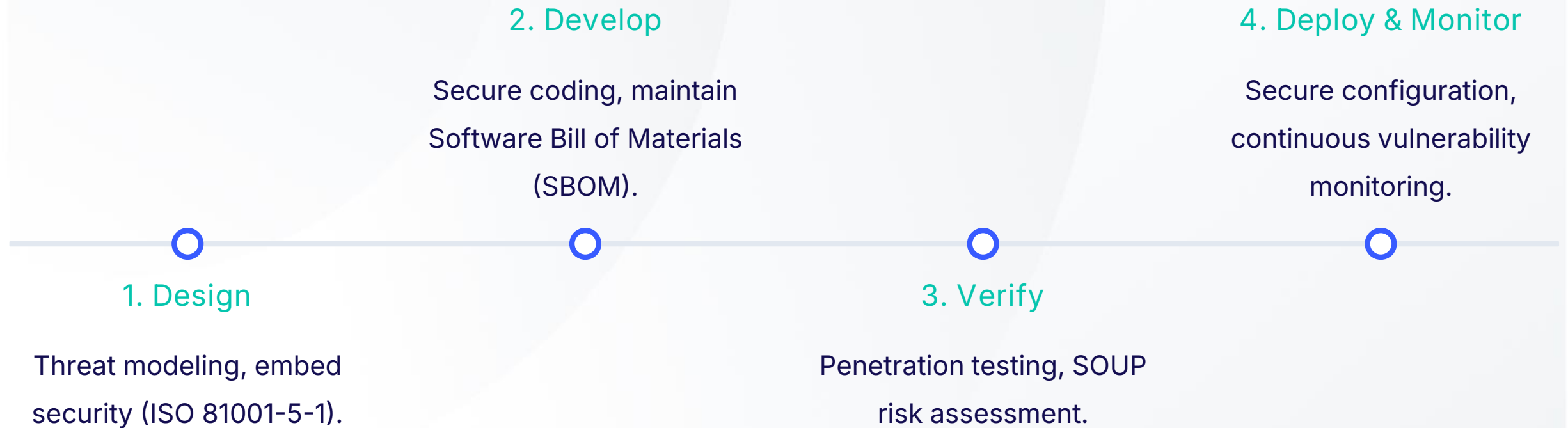
# Cybersecurity-by-Design

Embedding Security in MedTech



→ | [complianceandrisks.com](https://complianceandrisks.com)

# Security Across the Product Life-cycle



# Key Cybersecurity Legislation (US vs. EU)

## FDA (United States)

- FD&C Act (Sec. 524B): The legal foundation. Mandates SPDF, vulnerability monitoring, and postmarket plans.
- Patch Act: Legally requires manufacturers to have a plan to address postmarket vulnerabilities.
- FDA Premarket Guidance: The "how-to." Outlines submission rules, risk assessments, and SBOM requirements.

## European Union

- MDR/IVDR (GSPR 1): The foundation. Establishes the high-level requirement for security and risk management.
- Cyber Resilience Act (CRA): The "how-to." Mandates SBOMs, vulnerability handling, and 5-year support.
- NIS2 Directive: The reporting rule. Enforces 24-hour incident reporting and supply chain security.

# Key Cybersecurity Obligations: NIS2 & CRA

## NIS2 Directive

Applies to: 'Important Entities' (incl. MedTech).

Requires: Supply chain risk management, vulnerability handling.

Key Mandate: 24-hour initial reporting of significant incidents.

## Cyber Resilience Act (CRA)

- Applies to: All 'products with digital elements.'
- Requires: Security-by-design, vulnerability management.
- Key Mandates: Provide an **\*\*SBOM\*\***; **\*\*5 years\*\*** of post-market security support.



# Vulnerability & Incident Management

- A continuous, post-market obligation.
- Vulnerability Mgt: Proactive scanning, patching, and risk scoring (e.g., CVSS).
- Incident Reporting: Rapid reporting to authorities (NIS2) and users.
- TPLC Focus: Security risk management must cover the Total Product Life Cycle (TPLC).



# Cybersecurity in Asia: A Lifecycle Approach



## Lifecycle & Risk Focus

Most frameworks (e.g., Japan, S. Korea, Taiwan) mandate a full lifecycle approach, aligning with international standards like IEC 81001-5-1 and IEC 62304.



## Secure Design & Documentation

China's NMPA requires detailed cybersecurity registration files. Singapore and Japan mandate Software Bill of Materials (SBOM) for transparency.







## Unique National Frameworks

Singapore is introducing a tiered Cybersecurity Labelling Scheme (CLS). South Korea's "Digital Medical Products Act" creates a binding legal framework.



# Key Takeaways

-  AI is High-Risk: Most AI-driven MedTech is 'High-Risk' under the EU AI Act.
-  Dual Compliance: The EU requires compliance with \*both\* MDR/IVDR and the AI Act.
-  Security is Law: Cybersecurity-by-design is now a legal mandate (CRA, NIS2).
-  TPLC is Everything: Both AI governance and cybersecurity demand a Total Product Life Cycle approach.

# Data Protection and Governance



GDPR principles: lawfulness, minimization, accountability



Handling sensitive health data and vendor compliance



Cross-border data transfer and alignment with EHDS



# GDPR Principles: Lawfulness, Minimization, Accountability

## Cornerstone of digital health compliance

- With the General Data Protection Regulation (GDPR) as the foundation, and complemented by frameworks such as the European Health Data Space (EHDS) and AI Act, manufacturers, healthcare providers, and digital health innovators must ensure that the collection, processing, and sharing of health data are lawful, ethical, and secure.
- The GDPR (EU 2016/679) governs all processing of personal data, including health and genetic data, which are classified as special categories of data.
- Processing of health data must be based on a valid legal ground
- Under Article 5(1)(c), only data that are adequate, relevant, and limited to what is necessary for the intended purpose may be collected.
- GDPR requires that organizations demonstrate compliance, not just claim it.

This involves:

- Maintaining Records of Processing Activities (RoPA)
- Conducting Data Protection Impact Assessments (DPIAs) for high-risk processing (e.g., AI diagnostics)
- Appointing a Data Protection Officer (DPO) where required.
- Implementing technical and organizational measures (encryption, access control, audit logs).

# Handling Sensitive Health Data

Health data is among the most sensitive categories of personal information, requiring enhanced controls for confidentiality and integrity. It is classified as special category personal data under GDPR.

Stronger safeguards are required and key obligations include:

- Encryption at rest and in transit
- Robust access controls and authentication
- Pseudonymization or anonymization where possible
- Data retention limits aligned with regulatory and clinical needs

Medical devices that transmit or store health information (software, SaaS, cloud-connected devices) must demonstrate secure processing throughout the data lifecycle.



# Vendor Compliance

Manufacturers and healthcare organizations remain responsible even when using vendors.

This includes Cloud providers, Data analytics tools, Clinical trial platforms and others.

They must:

- Ensure Data Processing Agreements (DPAs) are in place
- Verify that sub-processors are disclosed and compliant
- Conduct vendor security assessments
- Ensure vendors follow GDPR and cybersecurity best practices
- Ensure the vendor supports patient rights (access, deletion, rectification)
- For high-risk processing, a DPIA is mandatory.



# Cross-Border Data Transfer and Alignment with EHDS

Digital health ecosystems often rely on cloud platforms, AI analytics, and international vendors, raising challenges under GDPR Chapter V.

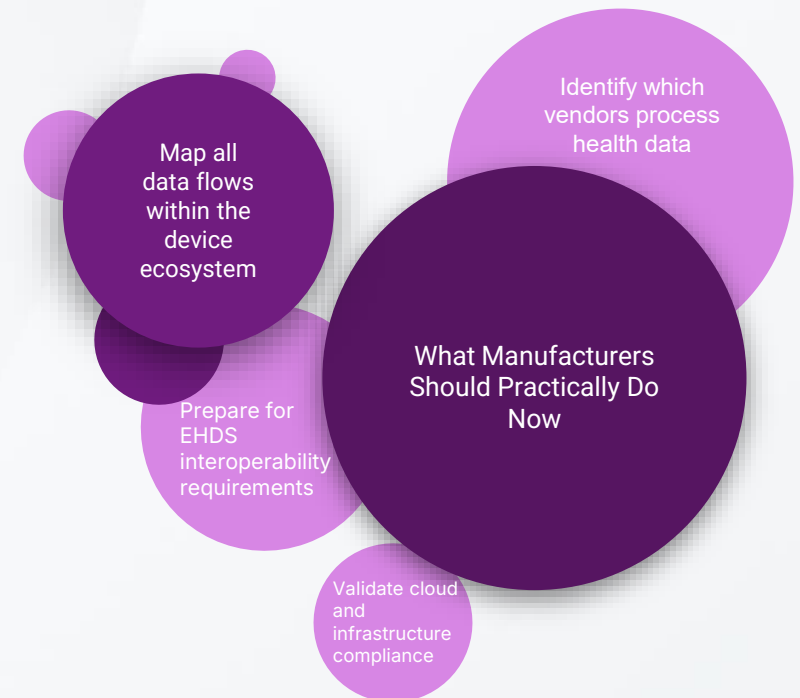
Under GDPR, personal data can only be transferred outside the EU/EEA in certain circumstances.

For medical devices with global cloud infrastructure, cross-border data flow must be:

- Transparent
- Documented
- Assessed for risk
- Aligned with Schrems II requirements (e.g., additional technical safeguards)

Last Update on 14th October 2025.

EU Factsheet - Patients Without Borders: Trend Analysis 2021-2023.  
Insights into EU Cross-Border Healthcare

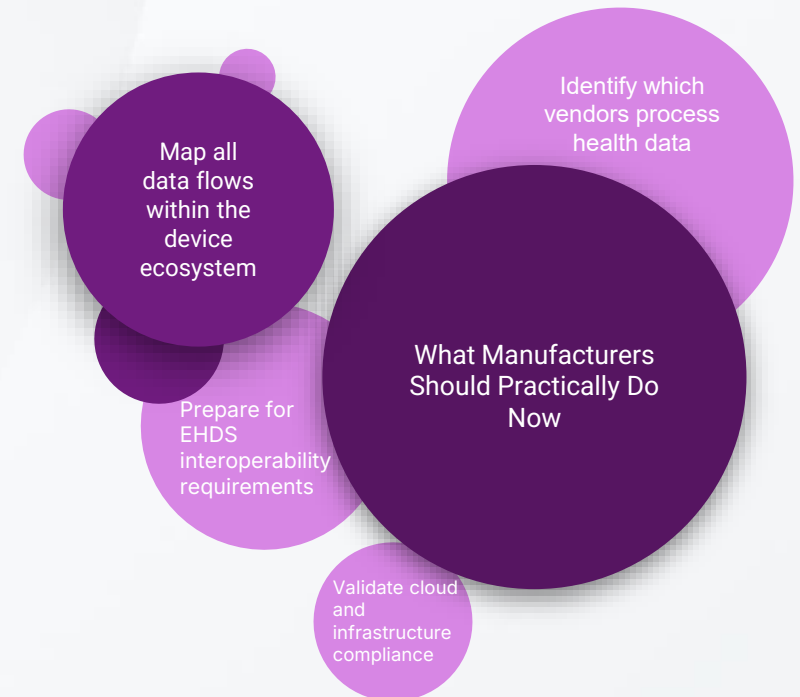


# Data Governance in Healthcare and MedTech

- Organizations must establish robust data governance frameworks, defining who can access which data, under what circumstances, and for what purposes.
- Use of interoperability standards (e.g., HL7 FHIR) should include built-in security and consent management functions.
- Any secondary use (e.g., AI training, clinical research, or post-market analysis) must ensure pseudonymization, ethical oversight, and purpose limitation.

It involves:

- ✓ Following GDPR principles
- ✓ Ensuring security and proper handling of sensitive health data
- ✓ Managing cross-border data transfers correctly
- ✓ Preparing for EHDS requirements

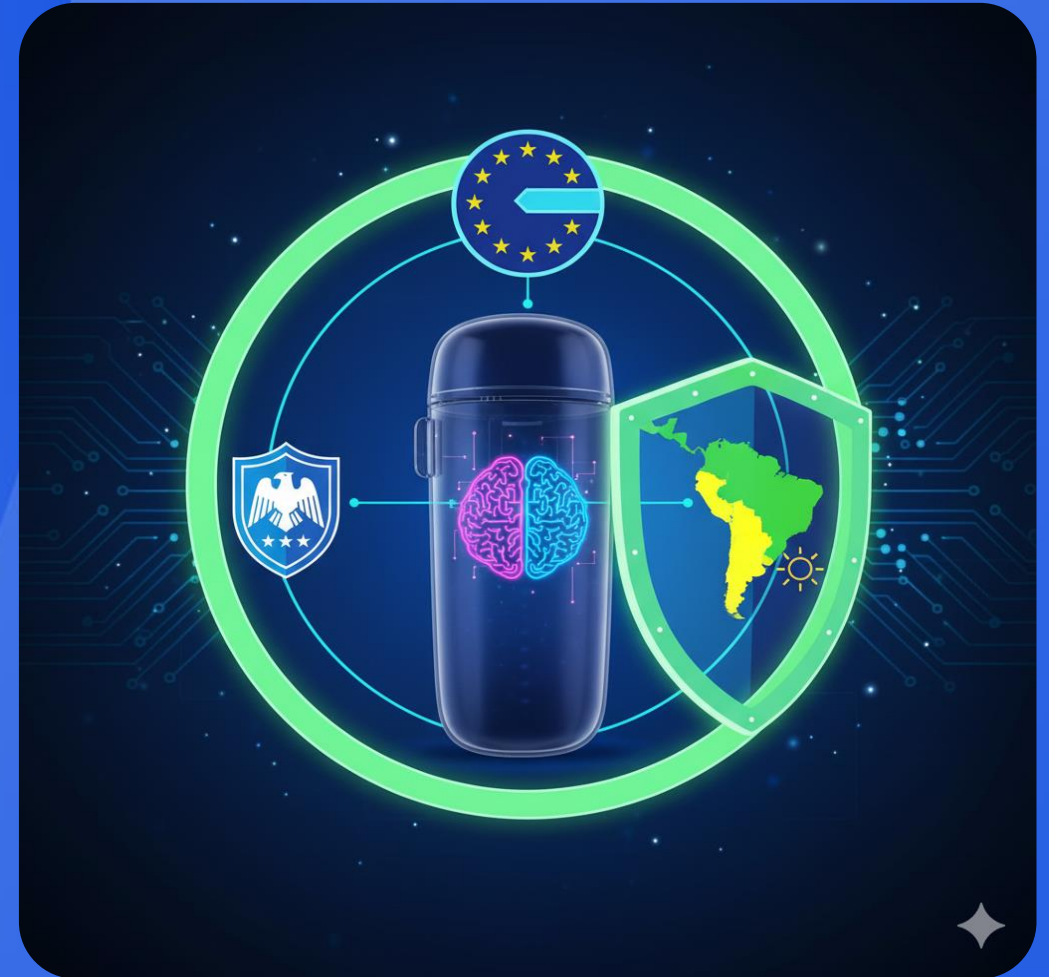


## 3 Compliance Strategies

- Integrating AI Governance & Data Protection
- Cross-Functional Compliance Frameworks
- Continuous Monitoring & Proactive Compliance

## 3 Regions

- Europe
- South America
- United States



# European Union Strategies

## Integrate AI Governance, Cybersecurity, & Data Protection

- MDR Annex 1 - General Safety & Performance Requirements (GSPR) Annex I (Section 17): requires AI or software to be designed and produced to include information security and unauthorized data access.
- EU AI Act (Article 10): mandates data quality requirements that are used to train, validate, and test AI systems thereby preventing algorithmic bias.
- GDPR: AI medical devices processing patient data must implement "Privacy by Design and Default" in systems and models.



# European Union Strategies

## Cross-Functional Compliance

- MDR Annex 1 - GSPR mandates comprehensive Quality and Risk Management systems which must establish cross-functional teams to regularly manage AI system's purpose, clinical performance, and safety.
- EU AI Act (Article 17): dedicated QMS for AI systems that is integrated into the MDR QMS. Cross-functional to cover data governance and human oversight.



# European Union Strategies

## Continuous Monitoring & Proactive Compliance

- Post-Market Surveillance (PMS) & Vigilance: Systematic PMS plan is required (MDR Article 83), along with reporting serious incidents (MDR Article 87). Monitoring for drift, bias, and security risks and applying CAPA.
- EU AI Act: Post-Market Monitoring (Article 61) and Log-keeping (Article 12) require that in addition to a plan for post-market monitoring, the AI system must automatically log its inputs and decisions for traceability, oversight, and corrective purposes. The focus here is accuracy, robustness, and cybersecurity (Article 15).



# South America Strategies

## Integrate AI Governance, Cybersecurity, and Data Protection

- Brazil (ANVISA) RDC No. 751/2022: Primary medical device regulation that includes rules for Software as Medical Device (SaMD) covers AI-enabled software, requiring manufacturers to prove safety, efficacy, and performance of algorithms.
- Brazil Law to Protect Personal Data (LGPD): Most critical South American regulation for data protection and AI governance (Article 20) - legal requirement for transparency.
- Peru Law No. 31814 (The AI Law): Risk-based approach for ethical, transparent AI use. Medical devices are High-Risk there by requiring mandatory human oversight, AI impact assessments.



# South America Strategies

## Cross-Functional Compliance

- Brazil 751: All devices must have a Medical Device Technical Dossier in their QMS to ensure cross-functional alignment on design, risk, and post-market processes.
- Brazil LGPD: Data protection specialists will work with engineering and quality teams during AI model training and monitoring.
- Peru Supreme Decree No. 115-2025: Requires use of cross-functional teams as part of compliance to Law 31814.



# South America Strategies

## Continuous Monitoring & Proactive Compliance

- Brazil 751: ANVISA requires technovigilance for complaints and adverse events - detecting issues and reporting drift or unexpected behavior during continuous monitoring.
- Peru Supreme Decree No. 115-2025: Requires monitoring as a mandatory phase of AI lifecycle to watch for drift and changes to patient population data that could affect product bias.



# United States Strategies

## Integrate AI Governance, Cybersecurity, and Data Protection

- Cybersecurity in Medical Devices: Quality System Considerations (Final): For the software bill of materials (SBOM) tangible deliverables are required for premarket submissions to mitigate supply chain risk and protect data.
- AI-Enabled Device Software Functions: Lifecycle Management requires transparency for users in AI models.
- Marketing Submission Recommendations for a PCCP (Final): Methodology for developing and validation changes to data management practices and AI retraining.



# United States Strategies

## Cross-Functional Compliance

- AI-Enabled Device Software Functions Total Product Lifecycle (TPLC) requires collaboration from design through post-market phases with particular attention to bias mitigation, transparency from data science, engineering and clinical teams.
- Cybersecurity in Medical Devices Secure Product Development Framework (SPDF) draft integration of security in design controls, so teams will do AI threat modeling.



# United States Strategies

## Continuous Monitoring & Proactive Compliance

- Cybersecurity in Medical Devices: Quality System Considerations (Final): Requires proactive plan to monitor, detect, and address vulnerabilities to include timely updates.
- Marketing Submission Recommendations for a PCCP (Final): The whole intent of PCCP is proactive compliance such as pre-authorized changes due to drift detection without another premarket submission.



# Table of Relevant Regulations and Laws

Jurisdiction	Primary Medical Device Law	Primary AI Law / Guidance	Overarching Data Privacy Law
European Union	Medical Device Regulation (MDR) 2017/745 and IVDR 2017/746.	Artificial Intelligence Act (AI Act) (Regulation (EU) 2024/1689). Classifies all medical AI as High-Risk.	General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
United States	Federal Food, Drug, and Cosmetic Act (FD&C Act) (governed by FDA CDRH).	AI/ML-Based Software as a Medical Device (SaMD) Action Plan and multiple FDA Guidance documents.	Health Insurance Portability and Accountability Act (HIPAA).
Argentina	Decree 1490/92 (ANMAT Authority) and ANMAT Provision 2319/02 (Classification, based on MERCOSUR).	Recommendations for Reliable AI (Provision 2/2023) (Soft Law, ethical principles). Bill 3003-D-2024 (Proposed AI Act).	Personal Data Protection Law (Law 25,326).
Brazil	ANVISA Resolution RDC No. 751/2022 (Harmonized with IMDRF/MDR).	Bill No. 2,338/2023 (Proposed National AI Act). ANVISA Technical Note on SaMD currently applies.	General Data Protection Law (LGPD) (Law 13,709/2018).
Chile	Sanitary Code Act and regulations by the ISP ( <i>Instituto de Salud Pública</i> ). Draft Decree to modernize MD/IVD regulation is pending.	Artificial Intelligence Bill (Introduced to Senate). Adopts an EU-style, risk-based approach with High-Risk categorization.	Law 19,628 (Data Protection Law, with modernization efforts underway).
Peru	Supreme Decree No. 016-2011-SA.	Law No. 31814 and its Regulation (Supreme Decree No. 115-2025-PCM) (Binding risk-based framework).	Personal Data Protection Law (Law No. 29733).
Mercosur (Regional Bloc)	MERCOSUR Resolution No. 40/00 (Medical Device Classification/ Registration).	None (AI regulation is handled at the national level).	None (Data protection is handled at the national level, though laws are often inspired by shared principles).



Compliance & Risks

# Future Trends & Regulatory Outlook



→ | [complianceandrisks.com](https://complianceandrisks.com)

# AI Act Enforcement Timeline and Ethical AI Requirements

The EU AI Act, adopted in 2024, is the world's first comprehensive law regulating artificial intelligence. It introduces a regulatory framework in addition to MDR/IVDR, not replacing them.

Its implementation will roll out in stages, allowing organizations to adapt gradually to its risk-based.

## Key Milestones:

- 2025: The AI Act formally enters into force, with provisions on prohibited AI practices taking effect within six months.
- 2026: Obligations for high-risk AI systems, including those used in medical devices and healthcare applications, become mandatory.
- 2027: Full enforcement expected - AI systems must comply with conformity assessment, documentation, transparency, and post-market monitoring requirements.

## Growing Focus on Ethical AI and Transparency

The regulatory focus is shifting beyond technical safety toward ethical governance of AI in healthcare.

## Key Trends:

Explainability and human oversight | Bias mitigation and representativeness | Ethical design and accountability | AI labeling and traceability

# Rising Cybersecurity Oversight and Audits

## What to Expect?

- More audits and supervisory inspections by competent authorities and notified bodies.
- Mandatory incident reporting within strict timelines under NIS2.
- Increased scrutiny of supply chain security, especially for AI models and cloud-based medical data services.

## The Future Role of Data Protection and Transparency in Innovation

- Data protection remains at the heart of digital health governance, and it is expanding beyond the GDPR to include sector-specific instruments.

### Key Developments:

- European Health Data Space (EHDS) development
- Cross-border data transfers
- Enhanced accountability
- Vendor and processor governance

Future compliance will depend not only on technical conformity but on demonstrable ethical responsibility and continuous risk management.

Organizations that embrace this proactive, integrated approach will be best positioned to lead the next era of trustworthy healthcare innovation.

# Questions?



# Lets Talk



---

Fernanda Paro  
Senior Regulatory  
Compliance Specialist



---

Patricia Weathers  
Regulatory  
Compliance Specialist



---

Kahyeon Seo  
Regulatory  
Compliance Analyst